【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/44862 A2

(51) International Patent Classification⁷: G06F

(21) International Application Number: PCT/US01/46688

(22) International Filing Date:
30 November 2001 (30.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/728,701 1 December 2000 (01.12.2000) US

(71) Applicant: NETWORK APPLIANCE, INC. [US/US]; 495 East Java Drive, Sunnyvale, CA 94089 (US).

(72) Inventor: MUHLESTEIN, Mark; 5831 E. Placita Alta Reposa, Tucson, AZ 85750 (US).

(74) Agent: SWERNOFSKY, Steven, A.; Swernofsky Law Group, P.O. Box 390013, Mountain View, CA 94039-0013 (US).

(81) Designated States *(national)*: CA, JP.

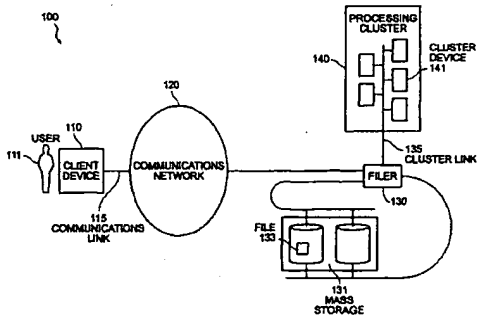
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: DECENTRALIZED APPLIANCE VIRUS SCANNING



(57) Abstract: The invention provides a method and system for scanning specialized computing devices for viruses. In a preferred embodiment, a filer is connected to one or more supplementary computing devices that scan requested files to ensure they are virus free prior to delivery to end users. When an end user requests a file the following steps occur: First, the filer determines whether the file requested must be scanned before delivery to the end user. Second, the filer opens a channel to one of the external computing devices and sends the filename. Third, the external computing device opens the file and scans it. Fourth, the external computing device notifies the filer the results of the file scan operation. Fifth, the filer sends the file to the end user provided the status indicates it may do so.

WO 02/44862 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

DECENTRALIZED APPLIANCE VIRUS SCANNING

Background of the Invention

1. *Field of the Invention*

This invention relates to virus scanning in a networked environment.

2. *Related Art*

Computer networking and the Internet in particular offer end users unprecedented access to information of all types on a global basis. Access to information can be as simple as connecting some type of computing device using a standard phone line to a network. With the proliferation of wireless communication, users can now access computer networks from practically anywhere.

Connectivity of this magnitude has magnified the impact of computer viruses. Viruses such as "Melissa" and "I love you" had a devastating impact on computer systems worldwide. Costs for dealing with viruses are often measured in millions and tens of millions of dollars. Recently it was shown that hand-held computing devices are also susceptible to viruses.

Virus protection software can be very effective in dealing with viruses, and virus protection software is widely available for general computing devices such as personal computers. There are, however, problems unique to specialized computing devices, such as filers (devices dedicated to storage and retrieval of data). Off-the-shelf virus protection software will not run on a specialized computing device unless it is modified to do so, and it can be very expensive to rewrite software to work on another platform.

A first known method is to scan for viruses at the data source. When the data is being provided by a specialized computing device the specialized computing device must be scanned. Device-specific virus protection software must be written in order to scan the files on the device.

While this first known method is effective in scanning files for viruses, it suffers from several drawbacks. First, a company with a specialized computing device would have to dedicate considerable resources to creating virus protection software and maintaining up-to-date data files that protect against new viruses as they emerge.

Additionally, although a manufacturer of a specialized computing device could enlist the assistance of a company that creates mainstream virus protection software to write the custom application and become a licensee this would create other problems, such as reliance on the chosen vendor of the anti-virus software, compatibility issues when hardware upgrades are effected, and a large financial expense.

A second known method for protecting against computer viruses is to have the end user run anti-virus software on their client device. Anti-virus software packages are offered by such companies as McAfee and Symantec. These programs are loaded during the boot stage of a computer and work as a backgroumd job monitoring memory and files as they are opened and saved.

While this second known method is effective at intercepting and protecting the client device from infection, it suffers from several drawbacks. It places the burden of detection at the last possible link in the chain. If for any reason the virus is not detected prior to reaching the end user it is now at the computing device where it will do the most damage (corrupting files and spreading to other computer users and systems).

It is much better to sanitize a file at the source from where it may be delivered to millions of end users rather than deliver the file and hope that the end user is prepared to deal with the file in the event the file is infected. End users often have older versions of anti-virus software and/or have not updated the data files that ensure the software is able to protect against newly discovered viruses, thus making detection at the point of mass distribution even more critical.

Also, hand-held computing devices are susceptible to viruses, but they are poorly equipped to handle them. Generally, hand-held computing devices have very limited memory resources compared to desktop systems. Dedicating a portion of these resources to virus protection severely limits the ability of the hand-held device to perform effectively. Reliable virus scanning at the information source is the most efficient and effective method.

Protecting against viruses is a constant battle. New viruses are created everyday requiring virus protection software manufacturers to come up with new data files (solution algorithms used by anti-virus applications). By providing protection at the source of the file, viruses can be eliminated more efficiently and effectively.

Security of data in general is important. Equally important is the trust of the end user. This comes from the reputation that precedes a company, and companies that engage in web commerce often live and die by their reputation. Just like an end user trusts that the credit card number they have just disclosed for a web-based sales transaction is secure they want files they receive to be just as secure.

Accordingly, it would be desirable to provide a technique for scanning specialized computing devices for viruses and other malicious or unwanted content that may need to be changed, deleted, or otherwise modified.

Summary of the Invention

The invention provides a method and system for scanning specialized computing devices (such as filers) for viruses. In a preferred embodiment, a filer is connected to one or more supplementary computing devices that scan requested files to ensure they are virus free prior to delivery to end users. When an end user requests a file from the filer the following steps occur: First, the filer determines whether the file requested must be scanned before delivery to the end user. Second, the filer opens a channel to one of the external computing devices and sends the filename. Third, the external computing device opens the file and scans it. Fourth, the external computing device notifies the filer the status of the file scan operation. Fifth, the filer sends the file to the end user provided the status indicates it may do so.

This system is very efficient and effective as a file needs only to be scanned one time for a virus unless the file has been modified or new data files that protect against new viruses have been added. Scan reports for files that have been scanned may be stored in one or more of the external computing devices, in one or more filers, and some portion of a scan report may be delivered to end users.

In alternative embodiments of the invention one or more of the external computing devices may be running other supplementary applications, such as file compression and encryption, independently or in some combination.

Brief Description of the Drawings

Figure 1 shows a block diagram of a system for decentralized appliance virus scanning.

Figure 2 shows a process flow diagram for a system for decentralized virus scanning

Detailed Description of the Preferred Embodiment

In the following description, a preferred embodiment of the invention is described with regard to preferred process steps and data structures. Those skilled in the art would recognize after perusal of this application that embodiments of the invention can be implemented using one or more general purpose processors or special purpose processors or other circuits adapted to particular process steps and data structures described herein, and that implementation of the process steps and data structures described herein would not require undue experimentation or further invention.

Lexicography

The following terms refer or relate to aspects of the invention as described below. The descriptions of general meanings of these terms are not intended to be limiting, only illustrative.

- **Virus** – in general, a manmade program or piece of code that is loaded onto a computer without the computer user's knowledge and runs against their wishes. Most viruses can also replicate themselves, and the more dangerous types of viruses are capable of transmitting themselves across networks and bypassing security systems.

- **client** and **server** — in general, these terms refer to a relationship between two devices, particularly to their relationship as client and server, not necessarily to any particular physical devices.

  For example, but without limitation, a particular client device in a first relationship with a first server device, can serve as a server device in a second relationship with a second client device. In a preferred embodiment, there are

generally a relatively small number of server devices servicing a relatively larger number of client devices.

- **client device** and **server device** — in general, these terms refer to devices taking on the role of a client device or a server device in a client-server relationship (such as an HTTP web client and web server). There is no particular requirement that any client devices or server devices must be individual physical devices. They can each be a single device, a set of cooperating devices, a portion of a device, or some combination thereof.

  For example, but without limitation, the client device and the server device in a client-server relation can actually be the same physical device, with a first set of software elements serving to perform client functions and a second set of software elements serving to perform server functions.

- **web client** and **web server** (or **web site**) — as used herein the terms "web client" and "web server" (or "web site") refer to any combination of devices or software taking on the role of a web client or a web server in a client-server environment in the internet, the world wide web, or an equivalent or extension thereof. There is no particular requirement that web clients must be individual devices. They can each be a single device, a set of cooperating devices, a portion of a device, or some combination thereof (such as for example a device providing web server services that acts as an agent of the user).

As noted above, these descriptions of general meanings of these terms are not intended to be limiting, only illustrative. Other and further applications of the invention, including extensions of these terms and concepts, would be clear to those of ordinary skill in the art after perusing this application. These other and further applications are part of the scope and spirit of the invention, and would be clear to those of ordinary skill in the art, without further invention or undue experimentation.

System Elements

Figure 1 shows a block diagram of a system for decentralized appliance virus scanning.

A system 100 includes a client device 110 associated with a user 111, a communications network 120, a filer 130, and a processing cluster 140.

The client device 110 includes a processor, a main memory, and software for executing instructions (not shown, but understood by one skilled in the art). Although the client device 110 and filer 130 are shown as separate devices there is no requirement that they be physically separate.

In a preferred embodiment, the communication network 120 includes the Internet. In alternative embodiments, the communication network 120 may include alternative forms of communication, such as an intranet, extranet, virtual private network, direct communication links, or some other combination or conjunction thereof.

A communications link 115 operates to couple the client device 110 to the communications network 120.

The filer 130 includes a processor, a main memory, software for executing instructions (not shown, but understood by one skilled in the art), and a mass storage 131. Although the client device 110 and filer 130 are shown as separate devices there is no requirement that they be separate devices. The filer 130 is connected to the communications network 120.

The mass storage 131 includes at least one file 133 that is capable of being requested by a client device 110.

The processing cluster 140 includes one or more cluster device 141 each including a processor, a main memory, software for executing instructions, and a mass storage (not shown but understood by one skilled in the art). Although the filer 130 and the processing cluster 140 are shown as separate devices there is no requirement that they be separate devices.

In a preferred embodiment the processing cluster 140 is a plurality of personal computers in an interconnected cluster capable of intercommunication and direct communication with the filer 130.

The cluster link 135 operates to connect the processing cluster 140 to the filer 130. The cluster link 135 may include non-uniform memory access (NUMA), or communication via an intranet, extranet, virtual private network, direct communication links, or some other combination or conjunction thereof.

Method of Operation

Figure 2 shows a process flow diagram for a system for decentralized appliance virus scanning.

A method 200 includes a set of flow points and a set of steps. The system 100 performs the method 200. Although the method 200 is described serially, the steps of the method 200 can be performed by separate elements in conjunction or in parallel, whether asynchronously, in a pipelined manner, or otherwise. There is no particular requirement that the method 200 be performed in the same order in which this description lists the steps, except where so indicated.

At a flow point 200, the system 100 is ready to begin performing the method 200.

At a step 201, a user 111 utilizes the client device 110 to initiate a request for a file 133. The request is transmitted to the filer 130 via the communications network 120. In a preferred embodiment the filer 130 is performing file retrieval and storage at the direction of a web server (not shown but understood by one skilled in the art).

At a step 203, the filer 130 receives the request for the file 133 and sends the file ID and path of the file 133 to the processing cluster 140 where it is received by one of the cluster device 141.

At a step 205, the cluster device 141 uses the file ID and path to open the file 133 in the mass storage 131 of the filer 130.

At a step 207, the cluster device 141 scans the file 133 for viruses. In a preferred embodiment, files are tasked to the processing cluster 140 in a round robin fashion. In alternative embodiments files may be processed individually by a cluster device 141, by multiple cluster device 141 simultaneously, or some combination thereof. Load balancing may be used to ensure maximum efficiency of processing within the processing cluster 140.

There are several vendors offering virus protection software for personal computers, thus the operator of the filer 130 may choose whatever product they would like to use. They may even use combinations of vendors' products in the processing cluster 140. In an alternative embodiment of the invention, continual scanning of every file 133 on the filer 130 may take place.

The processing cluster 140 is highly scalable. The price of personal computers is low compared to dedicated devices, such as filers, therefore this configuration is very desirable. Additionally, a cluster configuration offers redundant systems availability in case a cluster device 141 fails – failover and takeover is also possible within the processing cluster.

At a step 209, the cluster device 141 transmits a scan report to the filer 130. The scan report primarily reports whether the file is safe to send. Further information may be saved for statistical purposes (for example, how many files have been identified as infected, was the virus software able to sanitize the file or was the file deleted) to a database. The database may be consulted to determine whether the file 133 needs to be scanned before delivery upon receipt of a subsequent request. If the file 133 has not changed since it was last scanned and no additional virus data files have been added to the processing cluster, the file 133 probably does not need to be scanned. This means the file 133 can be delivered more quickly.

Other intermediary applications may also run separately, in conjunction with other applications, or in some combination thereof within the processing cluster 140. Compression and encryption utilities are some examples of these applications. These types of applications, including virus scanning, can be very CPU intensive, thus outsourcing can yield better performance by allowing a dedicated device like a filer to do what it does best and farm out other tasks to the processing cluster 140.

At a step 211, the filer 130 transmits or does not transmit the file 133 to the client 110 based on its availability as reported following the scan by the processing cluster 140. Some portion of the scan report may also be transmitted to the user.

At this step, a request for a file 133 has been received, the request has been processed, and if possible a file 133 has been delivered. The process may be repeated at step 201 for subsequent requests.

Generality of the Invention

The invention has wide applicability and generality to other aspects of processing requests for files.

The invention is applicable to one or more of, or some combination of, circumstances such as those involving:

- file compression;
- file encryption; and
- general outsourcing of CPU intensive tasks from dedicated appliances to general purpose computers.

Alternative Embodiments

Although preferred embodiments are disclosed herein, many variations are possible which remain within the concept, scope, and spirit of the invention, and these variations would become clear to those skilled in the art after perusal of this application.

Claims

1. A method for operating a filer including the steps of:

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes at least one of the following: (1) searching for one or more recognizable patterns of data within said object, (2) compressing said object, and (3) encrypting said object;

responding to said request, wherein said step of responding includes delivery of a response to said user.

2. The method of claim 1, wherein said request is in an electronic form.

3. The method of claim 1, wherein said object is a file.

4. The method of claim 3, wherein said step of processing said request further includes the steps of:

creating an access path from said filer to a processing cluster;

processing said file in said processing cluster; and

generating a scan report wherein, said scan report is responsive to said processing of said file in said processing cluster.

5. The method of claim 4, wherein said step of creating an access path includes sending the ID and path of said file from said filer to said processing cluster.

6. The method of claim 5, wherein said step of sending is accomplished using non-uniform memory access.

7. The method of claim 5, wherein said step of sending is accomplished using a communications network.

8. The method of claim 5, wherein said step of sending is accomplished using a direct connection.

9. The method of claim 4, wherein said step of processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

10. The method of claim 4, wherein said step of processing of said file is accomplished in parts by more than one device in said processing cluster.

11. The method of claim 4, wherein all files stored on said filer are scanned in a logical continuous manner.

12. The method of claim 4, wherein said scan report contains a set of status data relating to said processing of said file.

13. The method of claim 12, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

14. The method of claim 13, wherein said report is transferred to said filer.

15. The method of claim 14, wherein said report is stored in a first database.

16. The method of claim 15, wherein the necessity for subsequent scanning of said file is a function of determining whether said database contains said report relating to said file and whether said file has changed since last accessed.

17. The method of claim 16, wherein the necessity for subsequent scanning of said file is a function of determining whether additional virus identification data files have been added to said processing cluster.

18. The method of claim 1, wherein said delivery of a response is said file.

19. The method of claim 1, wherein said delivery of a response includes notification to said user that said file is unavailable.

20. The method of claim 1, wherein said step of responding to said request includes sending said user a copy of said scan report.

21. An apparatus for operating a filer including:

means for receiving at a first location a request from a user for an object;

means for processing said request at a second location, wherein said means for processing includes at least one of the following: (1) means for searching for one or more recognizable patterns of data within said object, (2) means for compressing said object, and (3) means for encrypting said object:

means for responding to said request, wherein said means for responding includes delivery of a response to said user.

22. The apparatus of claim 21, wherein said object is a file.

23. The apparatus of claim 22, wherein said means for processing said request further includes:

means for creating an access path from said filer to a processing cluster;

means for processing said file in said processing cluster; and

means for generating a scan report wherein, said scan report is responsive to said processing of said file in said processing cluster.

24. The apparatus of claim 23, wherein said means for creating an access path includes means for sending the ID and path of said file from said filer to said processing cluster.

25. The apparatus of claim 24, wherein said sending is accomplished using non-uniform memory access.

26. The apparatus of claim 24, wherein said sending is accomplished using a communications network.

27. The apparatus of claim 24, wherein said sending is accomplished using a direct connection.

28. The apparatus of claim 23, wherein said processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

29. The apparatus of claim 23, wherein said processing of said file is performed on atomic units of said file by more than one device in said processing cluster.

30. The apparatus of claim 23, wherein all files stored on said filer are scanned in a logical continuous manner.

31. The apparatus of claim 23, wherein said scan report contains a set of status data relating to said processing of said file.

32. The apparatus of claim 31, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

33. The apparatus of claim 31, wherein said report is transferred to said filer.

34. The apparatus of claim 33, wherein said report is stored in a first database.

35. The apparatus of claim 34, wherein the necessity for subsequent scanning of said file is a function of determining whether said database contains said report relating to said file and whether said file has changed since last accessed.

36. The apparatus of claim 35, wherein the necessity for subsequent scanning of said file is a function of determining whether additional virus identification data files have been added to said processing cluster.

37. The apparatus of claim 21, wherein said delivery of a response is delivery of said file.

38. The apparatus of claim 21, wherein said delivery of a response includes delivery of notification to said user that said file is unavailable.

39. The apparatus of claim 21, wherein said responding to said request includes sending said user some portion of said scan report.

40. A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving a request at a server for a file;

sending an identifier for the file to a scanning device that scans the file for viruses;

receiving an indication from the scanning device as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send.

41. A method as in claim 40, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

42. A method as in claim 40, wherein the request is received from and the file is sent to a client device.

43. A method as in claim 40, wherein the server is a web server.

44. A method as in claim 40, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

45. A method as in claim 44, wherein the cluster of devices is a cluster of interconnected personal computers.

46. A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

maintaining a database that indicates if files served by a server are safe to send from the server;

receiving a request at the server for a file;

if the database indicates that the file is safe to send, responding to the request by sending the file; and

if the database does not indicate that the file is safe to send, then sending an identifier for the file to a scanning device that scans the file for viruses, receiving an indication from the scanning device as to whether or not the file is safe to send from the server, and responding to the request by sending the file if the indication is that the file is safe to send.

47. A method as in claim 46, wherein maintaining the database further comprises the steps of:

tracking received indications from the scanning device; and

tracking accesses to the file.

48. A method as in claim 47, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

49. A method as in claim 46, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

50. A method as in claim 46, wherein the request is received from and the file is sent to a client device.

51. A method as in claim 46, wherein the server is a web server.

52. A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving from a server, at a scanning device connected to the server, an identifier for a file stored on mass storage for the server;

scanning the file for viruses; and

reporting an indication to the server as to whether or not the file is infected.

53. A method as in claim 52, further comprising the step of changing, deleting, or otherwise modifying the file based on a result of scanning the file for viruses.

54. A method as in claim 52, wherein the server is a web server.

55. A method as in claim 52, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

56. A method as in claim 55, wherein the cluster of devices is a cluster of interconnected personal computers.

57. A server that attempts to provide virus protection in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to receive a request for a file, (b) to send an identifier for the file to a scanning device that scans the file for viruses, (c) to receive an indication from the scanning device as to whether or not the file is safe to send from the server, and (d) to respond to the request by sending the file if the indication is that the file is safe to send.

58. A server as in claim 57, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

59. A server as in claim 57, wherein the request is received from and the file is sent to a client device.

60. A server as in claim 57, wherein the server is a web server.

61. A server as in claim 57, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

62. A server as in claim 61, wherein the cluster of devices is a cluster of interconnected personal computers.

63. A server that attempts to provide virus protection in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to maintain a database that indicates if files served by a server are safe to send from the server, (b) to receive a request at the server for a file, (c) if the database indicates that the file is safe to send, to respond to the request by sending the file, and (d) if the database does not indicate that the file is safe to send, then to send an identifier for the file to a scanning device that scans the file for viruses, to receive an indication from the scanning device as to whether or not the file is safe to send from the server, and to respond to the request by sending the file if the indication is that the file is safe to send.

64. A server as in claim 63, wherein the instructions to maintain the database further comprise instructions to track received indications from the scanning device, and to track accesses to the file.

65. A server as in claim 64, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

66. A server as in claim 63, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

67. A server as in claim 63, wherein the request is received from and the file is sent to a client device.

68. A server as in claim 63, wherein the server is a web server.

69. A scanning device that attempts to provide virus protection for a server in a client-server environment, comprising:

a communication link to the server; and

a processor that executes instructions, the instructions including instructions (a) to receive from the server an identifier for a file stored on mass storage for the server, (b) to scan the file for viruses, and (c) to report an indication to the server as to whether or not the file is infected.

70. A scanning device as in claim 69, wherein the instructions further comprise instructions to change, delete, or otherwise modify the file based on a result of scanning the file for viruses.

71. A scanning device as in claim 69, wherein the server is a web server.

72. A scanning device as in claim 69, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

73. A scanning device as in claim 72, wherein the cluster of devices is a cluster of interconnected personal computers.

74. Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving a request at a server for a file;

sending an identifier for the file to a scanning device that scans the file for viruses;

receiving an indication from the scanning device as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send.

75. Storage as in claim 74, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

76. Storage as in claim 74, wherein the request is received from and the file is sent to a client device.

77. Storage as in claim 74, wherein the server is a web server.

78. Storage as in claim 74, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

79. Storage as in claim 78, wherein the cluster of devices is a cluster of interconnected personal computers.

80. Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

maintaining a database that indicates if files served by a server are safe to send from the server;

receiving a request at the server for a file;

if the database indicates that the file is safe to send, responding to the request by sending the file; and

if the database does not indicate that the file is safe to send, then sending an identifier for the file to a scanning device that scans the file for viruses, receiving an indication from the scanning device as to whether or not the file is safe to send from the server, and responding to the request by sending the file if the indication is that the file is safe to send.

81. Storage as in claim 80, wherein maintaining the database further comprises the steps of:

tracking received indications from the scanning device; and

tracking accesses to the file.

82. Storage as in claim 81, wherein a tracked indication in the database that the file is safe to send is cancelled if the file has changed since the tracked indication was incorporated into the database.

83. Storage as in claim 80, wherein the scanning device indicates that the file is safe to send if the scanning device determines that the file is not infected with any viruses.

84. Storage as in claim 80, wherein the request is received from and the file is sent to a client device.

85. Storage as in claim 80, wherein the server is a web server.

86. Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving from a server, at a scanning device connected to the server, an identifier for a file stored on mass storage for the server;

scanning the file for viruses; and

reporting an indication to the server as to whether or not the file is infected.

87. Storage as in claim 86, wherein the instructions further comprise the step of changing, deleting, or otherwise modifying the file based on a result of scanning the file for viruses.

88. Storage as in claim 86, wherein the server is a web server.

89. Storage as in claim 86, wherein the scanning device is one of a cluster of devices connected to the server that function similarly to the scanning device.

90. Storage as in claim 89, wherein the cluster of devices is a cluster of interconnected personal computers.

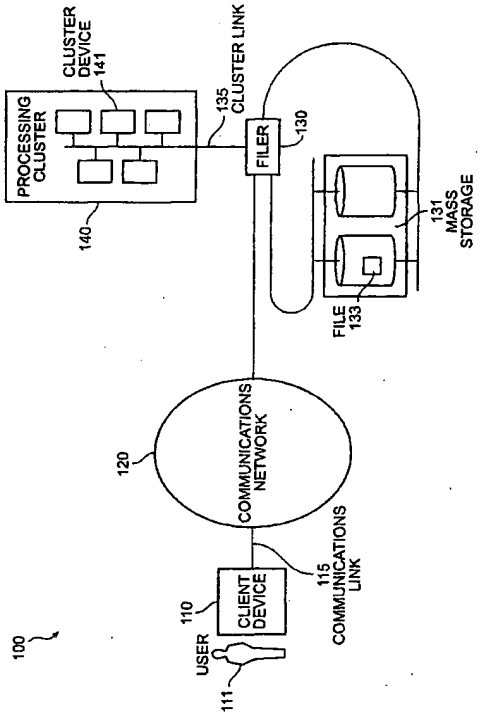

CLUSTER DEVICE 141
135 CLUSTER LINK
PROCESSING CLUSTER
140
FILER
130
131 MASS STORAGE
FILE 133
120
COMMUNICATIONS NETWORK
115 COMMUNICATIONS LINK
110
CLIENT DEVICE
USER
111
100

FIG. 1

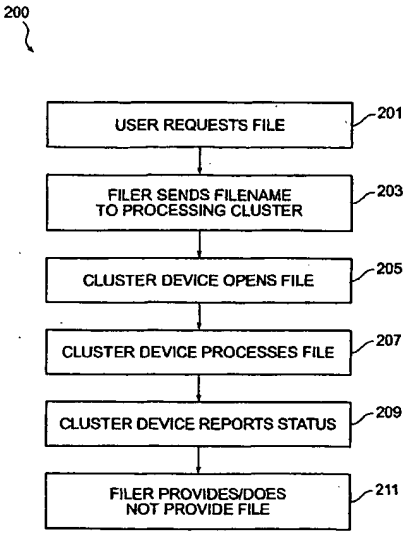

200
USER REQUESTS FILE
201
FILER SENDS FILENAME TO PROCESSING CLUSTER
203
CLUSTER DEVICE OPENS FILE
205
CLUSTER DEVICE PROCESSES FILE
207
CLUSTER DEVICE REPORTS STATUS
209
FILER PROVIDES/DOES NOT PROVIDE FILE
211

FIG. 2

【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 June 2002 (06.06.2002)

PCT

(10) International Publication Number
WO 02/044862 A3

(51) International Patent Classification⁷: G06F 7/00, 11/34

(21) International Application Number: PCT/US01/46688

(22) International Filing Date:
30 November 2001 (30.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/728,701 1 December 2000 (01.12.2000) US

(71) Applicant: NETWORK APPLIANCE, INC. [US/US]; 495 East Java Drive, Sunnyvale, CA 94089 (US).

(72) Inventor: MUHLESTEIN, Mark; 5831 E. Placita Alta Reposa, Tucson, AZ 85750 (US).

(74) Agent: SWERNOFSKY, Steven, A.; Swernofsky Law Group, P.O. Box 390013, Mountain View, CA 94039-0013 (US).

(81) Designated States *(national)*: CA, JP.

(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

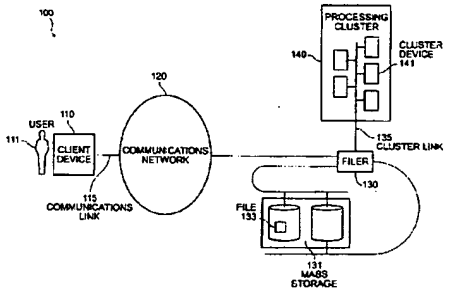
Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*

Published:
— *with international search report*

(88) Date of publication of the international search report:
30 May 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DECENTRALIZED APPLIANCE VIRUS SCANNING



(57) Abstract: The invention provides a method and system for scanning specialized computing devices for viruses. In a preferred embodiment, a filer (130) is connected to one or more supplementary computing devices (140) that scan requested files to ensure they are virus free prior to delivery to end users. When an end user (111) requests a file the following steps occur: First, the filer determines whether the file requested must be scanned before delivery to the end user. Second, the filer opens a channel to one (141) of the external computing devices and sends (203) the filename. Third, the external computing device opens (205) the file and scans (207) it. Fourth, the external computing device notifies the filer the results of the file scan operation. Fifth, the filer sends (211) the file to the end user provided the status indicates it may do so.

WO 02/044862 A3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/46538

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :G06F 7/00, 11/34
US CL : 713/188, 200, 201; 707/6
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/188, 200, 201; 707/6

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST
search terms: computer, virus, database, server, filer

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,088,803 A (TSO et al.) 11 July 2000, Abstract, Figures 1 and 2.	1, 2 , 3, 18-21 and 37-39 --- 4-17, 22-36 and 40-90
Y	US 5,392,446 A (TOWER et al.) 21 February 1995, Abstract, Fig. 2, columns 1-5.	4-17, 22-36 and 40-90
Y	US 6,101,558 A (ATSUNOMIYA et al) 08 August 2000, Abstract, Figure 1.	4-17, 22-36 and 40-90
Y	US 5,918,008 A (TOGAWA et al.) 29 June 1999, Abstract and Figures.	46-51, 53-68 and 80-85.

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 JULY 2002	07 AUG 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LY V. HUA Telephone No. (703) 305-9684

Form PCT/ISA/210 (second sheet) (July 1998)*